HIPAA

SECURITY STANDARDS

A Guide to Security Readiness

The MARYLAND HEALTH CARE COMMISSION

Rex W. Cowdry, M.D.
Executive Director

Revised October 2009

Commissioners

Marilyn Moon, Ph.D., Chair
Vice President and Director, Health Program
American Institutes for Research

Garret A. Falcone, Vice Chair
Executive Director
Charlestown Retirement Community

Reverend Robert L. Conway
Retired Principal and Teacher
Calvert County Public School System

John E. Fleig, Jr.
Director
United Healthcare

Tekedra McGee Jefferson, Esquire
Assistant General Counsel
AOL LLC

Kenny W. Kan
Senior Vice President/Chief Actuary
CareFirst BlueCross BlueShield

Sharon Krumm, R.N., Ph.D.
Administrator & Director of Nursing
The Sidney Kimmel Cancer Center
Johns Hopkins Hospital

Robert Lyles, Jr., M.D.
Medical Director
LifeStream Health Center

Barbara Gill McLean, M.A.
Retired, Senior Policy Fellow
University of Maryland School of Medicine

Roscoe M. Moore, Jr., D.V.M., Ph.D., D.Sc.
Retired, U.S. Department of Health
and Human Services

Kurt B. Olsen, Esquire
Klafter and Olsen LLP

Sylvia Ontaneda-Bernales, Esquire
Ober, Kaler, Grimes, & Shriver

Darren W. Petty
President
Maryland State United Auto Workers
General Motors/United Auto Workers

Nevins W. Todd, Jr., M.D.
Cardiothoracic and General Surgery
Peninsula Regional Medical Center

Randall P. Worthington
President/Owner
York Insurance Services, Inc.

INTRODUCTION

The Maryland Health Care Commission developed, *"A Guide to Security Readiness"* with the assistance of the EDI/HIPAA Workgroup. The purpose of this document is to promote the adoption of the HIPAA security standards among health care providers in Maryland. Users of the guide are encouraged to implement the security standards in a manner that is reasonable and consistent with their organizational structure. The contents of this guide represent leading best practices relating to implementation. *Users of the guide are encouraged to review the regulations at* http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf *for more specific information on the HIPAA regulations.*

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires payers, providers, and claims clearinghouses (covered entities) to adopt the security standards in order to ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) that they create, receive, maintain, or transmit.

The security standards are designed to protect the integrity of EPHI from any reasonably anticipated threats or hazards; they are organized into three sections referred to as safeguards: administrative, physical, and technical. Each safeguard is further defined by standards. Administrative safeguards contain nine standards, physical safeguards contain four standards, and technical safeguards contain five standards. Most of the standards are further defined by implementation specifications.

The Office of Civil Rights (OCR) within the Department of Health and Human Services (DHHS) is responsible for enforcing the security standards. Enforcement is expected to be complaint-driven.

A New Concept - Required & Addressable

The implementation specifications are separated into *required* or *addressable* categories. A *required* implementation specification must be implemented. An *addressable* implementation specification allows covered entities to select from those that seem reasonable to the organization or to implement an appropriate *alternative* protection. If an organization determines that an addressable implementation specification is not "*reasonable and appropriate*," the organization must *document* the reason the implementation specification is not reasonable and appropriate. Organizations must implement an equivalent *alternative* measure if doing so is determined to be reasonable and appropriate.

Organizations must take into account size, complexity, technical infrastructure, hardware, software, and the costs of adopting the security measures. The level of adoption is largely driven by potential risks to the EPHI.

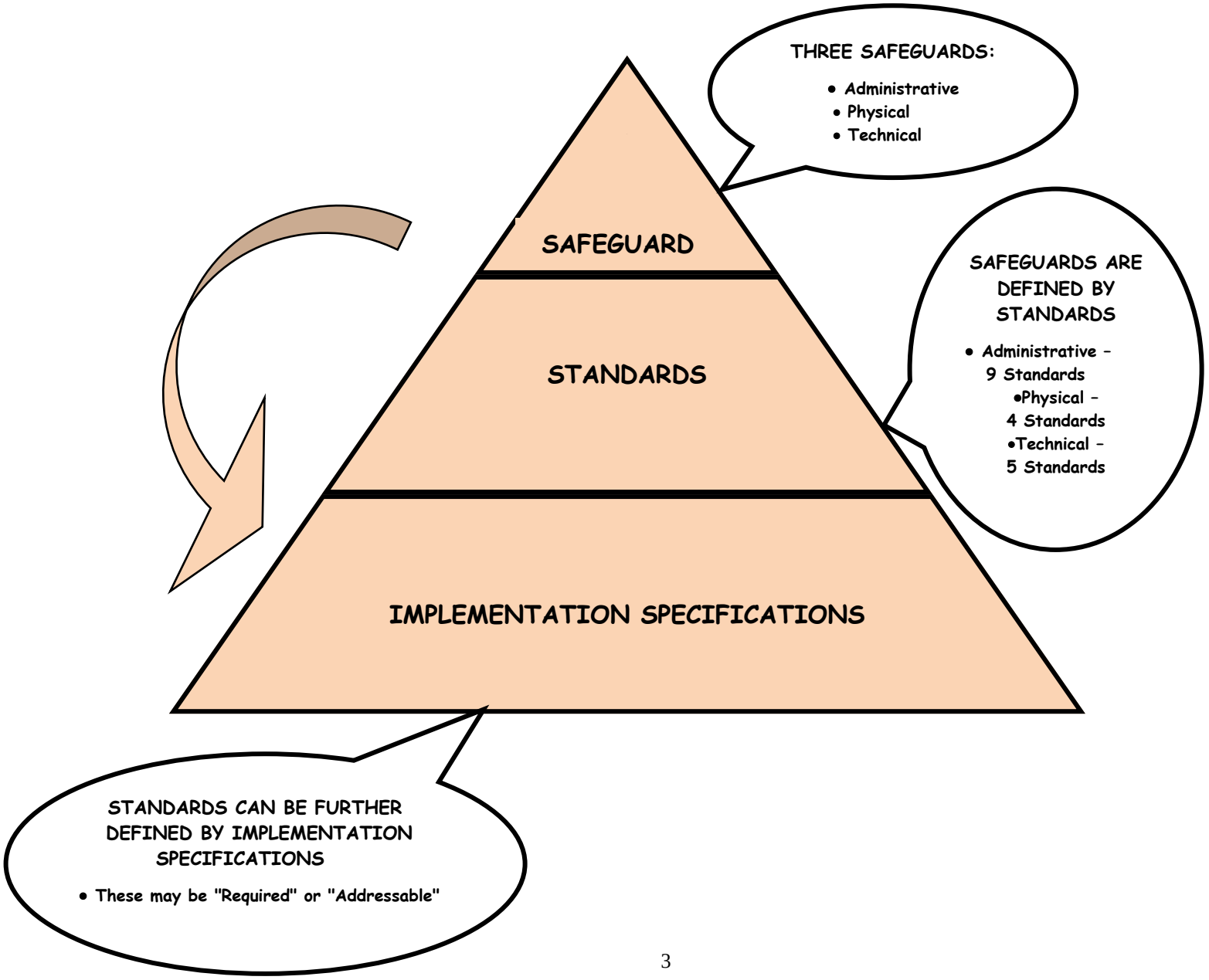
Documentation Requirements

Providers are required to maintain written policies and procedures of any action, activity, or assessment required by the standard. Documentation must be retained for six years from the date that it was created or was last in effect, whichever is later.

Providers must make this documentation available to its workforce. Policies and procedures should be reviewed and updated periodically or as needed in response to environmental or operational changes that may affect the security of EPHI.

THE HIPAA SECURITY REGULATION

Illustration



Specification & Content Table

Specification table includes:

SUMMARY TABLE

- Security categories & components

Safeguards & Standards Chart

Safeguards		
Administrative	***Physical***	***Technical***
Standards		
1. Security Management Process	**1. Facility Access Controls**	**1. Access Control**
2. Assigned Security Responsibility	**2. Workstation Use**	**2. Audit Controls**
3. Workforce Security	**3. Workstation Security**	**3. Integrity**
4. Information Access Management	**4. Device & Media Controls**	**4. Person or Entity Authentication**
5. Security Awareness & Training		**5. Transmission Security**
6. Security Incident Procedures		
7. Contingency Plan		
8. Evaluation		
9. Business Associate Contracts & Other Arrangement		

Content table includes:

- Safeguard that the standard defines
- Regulation citation number
- An ***R*** or an ***A*** next to each implementation specification indicating **Required** or **Addressable**
- Action items and assessment questions
- Interactive questions

Example
Physical Safeguards
§164.310 (d) (1) DEVICE AND MEDIA CONTROLS

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N= No SW = Somewhat		
R ***NAME A SECURITY OFFICIAL*** **§164.308 (a) (2)** • **Identify** a security official within your organization who is responsible for implementation and developing policies and procedures **? Have you identified a security official ?**	☐ **Yes**	☐ **No**	☐ **SW**
R ***DOCUMENT SECURITY OFFICIAL RESPONSIBILITIES*** **§164.308 (a) (2)** • **Update** their job description to include policies and procedures development and security implementation • **Identify** duties of the security official • **Communicate** security official responsibilities to workforce **? Do you have a job description that outlines specific security duties ?**	☐ **Yes**	☐ **No**	☐ **SW**

STANDARD INFORMATION

- Safeguard category
- HIPAA regulation reference number
- Explanation of Standard

IMPLEMENTATION SPECIFICATIONS & QUESTIONS

- ⓘ introduces Action Items & Assessment Questions
- Compliance category stated in laymen terms
- Suggested activities and general compliance question

Key Security Terms

Term	Description
Access	The ability to read, write, modify, or communicate using electronic protected healthcare information.
Addressable Implementation Specification	An element of the security standard that may be implemented if deemed reasonable and appropriate. Specifications not considered reasonable and appropriate requires supporting documentation and the implementation of an alternative measure if reasonable and appropriate.
Administrative Safeguards	Administrative actions including policies and procedures used to manage the selection, development, implementation, and maintenance of security measure to protect EPHI.
Authentication	A process used to validate an entity as originator or receiver of information.
Availability	Information accessible and useable upon demand by authorized personnel.
Biometrics	Identification system that measures human physical features of an individual that includes hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voiceprints, and handwritten signature.
Confidentiality	Protections used to maintain information so that it is not made available or disclosed to unauthorized persons or processes.
Contingency Plan	A response strategy to an information technology system disruption or facility disaster or emergency situation.
Data Backup	A retrievable exact copy of electronic information.
Disclosure	Releasing, transferring, providing or giving access to protected health information, including electronic protected health information (EPHI).
Electronic Media	Includes electronic storage media and transmission media.
Electronic Protected Health Information (EPHI)	Protected Health Information (PHI) that is transmitted by electronic media or maintained in electronic media.
Electronic Storage Media	A form of electronic media that includes computer hard drives, magnetic tapes or disks, optical disks, floppy disks, or memory cards.
Encryption	Transforming confidential plain text into cipher text making it unintelligible for storage and/or transmission over unsecured lines.
Facility	Refers to the physical premises where EPHI is located, and includes the interior and exterior of a building.
Information System	An interconnected set of information technology resources that shares a common functionality.
Integrity	A process that ensures electronic information has not been accidentally or deliberately altered in an unauthorized manner.
Malicious Software	Software used to damage or disrupt an information technology system(s).

Term	Description
Password	Confidential authentication information composed of a string of characters.
Physical Access Controls	Formal policies and procedures used to limit physical access while ensuring that properly authorized access is allowed.
Physical Safeguards	Formal policies, and procedures to protect electronic information systems, related buildings and equipment from unauthorized intrusion, and natural and environmental hazards.
Personal Identification Number (PIN)	A number or code assigned to an individual used to provide user identify verification.
Required Implementation Specification	An implementation specification that must be implemented in order to be compliant with the security standards.
Role-Based Access Control	Access to a computer system or application assigned based on job function.
Security or Security Measures	Administrative, physical, and technical safeguards in an information technology system.
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information technology system. This can include violations by an employee or other individual, intrusion by virus or outside entity into your computer system, or a security breach of EPHI that is being transmitted to an outside entity.
Technical Safeguards	Formal policy and procedures used to protect information technology and limit access.
Transmission Media	The process that is used to exchange electronic information including the internet, extranet, leased lines, dial-up lines (via modem), private networks, or moving removable/transportable electronic storage media.
User	A person or entity authorized to access an information technology system or application.
User-Based Access	Access to information technology system(s) or application(s) assigned on a user basis, by specifically detailing what information and what activities a user is permitted to access.
Workstation	An electronic computing device such as a laptop or desktop computer used to access and or exchange electronic information.

Administrative Safeguards

§164.308 (a) (1) (i) SECURITY MANAGEMENT PROCESS – Standard 1

Providers are required to implement policies and procedures to prevent, detect, contain, and correct security violations.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***CONDUCT A RISK ANALYSIS*** **§164.308 (a) (1) (ii) (A)**			
• **Inventory** all hardware and software systems used to collect, store, process, or transmit EPHI			
• **Identify** potential threats and weaknesses that include natural (fire), human (accidental or intentional corruption or loss of EPHI), and environmental threats (loss of electric power)			
• **Determine** whether controls (safeguards and countermeasures) are already in place to protect information technology systems for each identified threat or weakness			
? Have you completed your risk analysis ?	☐ Yes	☐ No	☐ SW
R ***MANAGE YOUR RISK*** **§164.308 (a) (1) (ii) (B)**			
• **Use** results from your risk analysis to determine controls required to protect your EPHI			
• **Implement** measures to protect EPHI where vulnerabilities exist			
? Have you implemented measures to limit your risks to EPHI ?	☐ Yes	☐ No	☐ SW
R ***SANCTION WORKFORCE VIOLATIONS*** **§164.308 (a) (1) (ii) (C)**			
• **Develop** sanctions for workforce members who violate security measures			
• **Conduct** security training sessions with workforce members			
? Do you sanction workforce member for security violations ?	☐ Yes	☐ No	☐ SW
R ***REVIEW SECURITY RELEVANT SYSTEM ACTIVITY*** **§164.308 (a) (1) (ii) (D)**			
• **Identify** the types of user activity which may be inappropriate or malicious			
• **Review** records of information system activity such as audit logs, access logs, and security incident tracking reports			
• **Document** system reviews and security relevant events			
? Do you review system activity records ?	☐ Yes	☐ No	☐ SW

Administrative Safeguards

§164.308 (a) (2) ASSIGNED SECURITY RESPONSIBILITY – Standard 2

Identify the security official who is responsible for the development and implementation of security policies and procedures

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***NAME A SECURITY OFFICIAL*** **§164.308 (a) (2)** • **Identify** a security official within your organization who is responsible for implementation and developing policies and procedures • **Update** their job description to include policies and procedures development and security implementation • **Communicate** security official responsibilities to workforce			
? Have you identified a security official ?	☐ **Yes**	☐ **No**	☐ **No**
R ***DOCUMENT EPHI ACCESS PROCEDURES*** **§164.308 (a) (2)** • **Update** policies and procedures on the steps required to gain access to EPHI • **Train** staff on access requirements • **Review** policies and procedures periodically for completeness as changes in staffing occur			
? Do you have a job description that outlines specific security duties ?	☐ **Yes**	☐ **No**	☐ **SW**

Administrative Safeguards

§164.308 (a) (3) (i) WORKFORCE SECURITY – Standard 3

Implement policies and procedures to ensure that all members of the workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to EPHI.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
A ***IMPLEMENT PROCEDURES TO AUTHORIZE/SUPERVISE EMPLOYEE ACCESS TO EPHI*** **§164.308 (a) (3) (ii) (A)**			
• **Determine** workforce required to access EPHI based upon job responsibilities • **Periodically** review workforce EPHI access and location requirements			
? Do you periodically review workforce EPHI access requirements ?	☐ Yes	☐ No	☐ SW
A ***DEVELOP A FORMAL PROCESS TO DETERMINE HOW EMPLOYEES ACCESS EPHI*** **§164.308 (a) (3) (ii) (B)**			
• **Determine** EPHI access requirement needs of your workforce • **Establish** document, review, and modify a user's right of access to workstation, transactions, and programs			
? Does a formal process exist that identifies users requiring access to EPHI ?	☐ Yes	☐ No	☐ SW
A ***IMPLEMENT PROCEDURES TO PREVENT ACCESS TO EPHI BY TERMINATED EMPLOYEES*** **§164.308 (a) (3) (ii) (C)**			
• **Implement** steps to collect physical access keys and block information technology access of terminated workforce			
? Do you have documented procedures for preventing terminated workforce access to computer system(s) ?	☐ Yes	☐ No	☐ SW

Administrative Safeguards

§164.308 (a) (4) (i) INFORMATION ACCESS MANAGEMENT – Standard 4

Implement policies and procedures for authorizing access to EPHI.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
A ***ACCESS AUTHORIZATION*** **§164.308 (a) (4) (ii) (B)**			

• **Identify** a method for workforce access to EPHI that is appropriate for your organization
  ○ *Role-based* access - Access by job requirements or description
  ○ *User-based access* - Access determined by specific user
  ○ *Location-based access* **-** Access defined by job location
• **Determine** individuals who can add, update, or delete EPHI from your information technology system(s)			

? Do you grant workforce access to EPHI using a consistent method ?	☐ **Yes**	☐ **No**	☐ **SW**

A ***ACCESS ESTABLISHMENT AND MODIFICATION*** **§164.308 (a) (4) (ii) (B)**
• **Determine** the appropriate workforce qualifications for accessing and making changes to EPHI
• **Implement** EPHI access procedure to include:
  ○ *Access management procedures* which can be enforced within existing office systems and networks
  ○ *Training program* for employees
  ○ *Ongoing review*			

? Does someone in your organization oversee EPHI access guidelines ?	☐ **Yes**	☐ **No**	☐ **SW**

Administrative Safeguards

§164.308 (a) (5) (i) SECURITY AWARENESS AND TRAINING – Standard 5

Implement a security awareness and training program for all members of your workforce, including management.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes	N = No	SW = Somewhat
A ***PROVIDE WORKFORCE SECURITY TRAINING WITH PERIODIC SECURITY REMINDERS*** **§164.308 (a) (5) (ii) (A)**			
• **Implement** security awareness training for all new and existing workforce that includes periodic refresher training • **Distribute** information aimed at reducing the risk of improper access, uses, and disclosures of EPHI to your workforce			
? Do you provide your workforce with initial and refresher training on protecting your computer system(s) ?	☐ Yes	☐ No	☐ SW
A ***PROTECT YOUR COMPUTER SYSTEMS FROM VIRUSES OR OTHER MALICIOUS SOFTWARE*** **§164.308 (a) (5) (ii) (B)**			
• **Define** appropriate workforce procedures relating to Internet use • **Check** all software for potential viruses before installation on workstations • **Install** virus protection software and review to make certain that you are using the latest version			
? Do you run virus protection software on your computer system(s) ?	☐ Yes	☐ No	☐ SW
A ***DEVELOP A PROCEDURE TO MONITOR & REPORT UNSUCCESSFUL LOG-IN ATTEMPTS*** **§164.308 (a) (5) (ii) (C)**			
• **Determine** if your computer system(s) blocks repeated failed user login attempts • **Review** your information technology system(s) for available reporting features on unsuccessful user logins			
? Can you track failed user login attempts ?	☐ Yes	☐ No	☐ SW
A ***IMPLEMENT PASSWORD MANAGEMENT PROCEDURES*** **§164.308 (a) (5) (ii) (D)**			
• **Establish** procedures for creating, changing, and safeguarding passwords			
? Do you instruct your workforce to use a combination of alpha numeric and special characters when selecting a password ?	☐ Yes	☐ No	☐ SW

Administrative Safeguards

§164.308 (a) (6) (i) SECURITY INCIDENT PROCEDURES – Standard 6

Implement policies and procedures to address security incidents.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***RESPONSE AND REPORTING*** **§164.308 (a) (6) (ii)** • **Develop** measures to address unauthorized computer system(s) access, use, disclosure, modification, or destruction of EPHI • **Evaluate** various response scenarios to lessen or remove the potential for future security breaches • **Track** responses to security breaches • **Identify** who should be informed when an actual or potential security breach occurs			
? Are you able to identify and appropriately respond to computer security breaches ?	☐ **Yes**	☐ **No**	☐ **SW**

Administrative Safeguards

§164.308 (a) (7) (i) CONTINGENCY PLAN – Standard 7

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***ESTABLISH AND IMPLEMENT A DATA BACKUP PROCEDURE*** **§164.308 (a) (7) (ii) (A)**			
• **Identify** computer system(s), programs, and/or data containing EPHI • **Implement** daily, weekly, or monthly backups as deemed appropriate by your organization • **Assign** backup duties to a designated workforce member and identify at least one alternate			
? Have you established & implemented data backup procedures ?	☐ Yes	☐ No	☐ SW
R ***DOCUMENT STEPS TO RECOVER LOST DATA (A DISASTER RECOVERY PLAN)*** **164.308 (a) (7) (ii) (B)**			
• **Develop** step-by-step procedures to restore your computer system(s) in the event of lost data			
? Do you have a documented disaster recovery plan ?	☐ Yes	☐ No	☐ SW
R ***DEVELOP & IMPLEMENT PROCEDURES TO CONTINUE OPERATIONS IN EMERGENCY MODE*** **§164.308 (a) (7) (ii) (C)**			
• **Identify** critical business operations such as patient scheduling, billing, etc., that would need to continue in the event of a disaster • **Identify** an alternate computer system(s) and location that can be used in the event of physical or system related disaster			
? Do you have documented procedures for operating in an emergency ?	☐ Yes	☐ No	☐ SW
A ***IMPLEMENT INITIAL AND PERIODIC TESTING & REVISION OF YOUR CONTINGENCY PLAN*** **§164.308 (a) (7) (ii) (D)**			
• **Test** on a routine basis your data backup, data recovery, and emergency mode operation procedures • **Identify** and resolve any problems that occur during the testing phase • **Revise** your data backup, data recovery, and emergency mode operation plan as changes occur in your physical resources and computer system(s)			
? Do you know what to do in the event of a computer system failure ?	☐ Yes	☐ No	☐ SW

Administrative Safeguards

§164.308 (a) (7) (i) CONTINGENCY PLAN – Standard 7 (*continued*)

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
A ***ASSESS ALL CRITICAL DATA SYSTEMS OR OFFICE PROCEDURES*** **§164.308 (a) (7) (ii) (E)** • **Determine** the overall importance of specific applications that support your contingency plan **? Are you aware of critical applications essential to your contingency plan ?**	☐ Yes	☐ No	☐ SW

Administrative Safeguards

§164.308 (a) (8) EVALUATION – Standard 8

Perform a periodic technical and non-technical evaluation, based initially on the security standards you have developed, and subsequently in response to environmental or operational changes affecting the security of EPHI.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***DETERMINE WHO WILL CONDUCT YOUR SECURITY EVALUATION*** **§164.308 (a) (8)** • **Select** an evaluation tool that will assist in completing a security evaluation of your information technology system(s) and physical resources • **Complete** a security review of your information technology system and physical resources prior to April 21, 2005 and thereafter when changes • **Periodically** assess your security adequacy as changes to your physical resources and information technology system(s) occur			
? Have you completed a security evaluation to assess environmental and operational conditions that affect EPHI ?	☐ **Yes**	☐ **No**	☐ **SW**

Administrative Safeguards

§164.308 (8) (b) (1) Business Associate Contracts and Other Arrangement – Standard 9

A covered entity may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***DETERMINE WHICH VENDORS REQUIRE A BUSINESS ASSOCIATE CONTRACT*** **§164.308 (b) (1)** • **Identify** trading partners that create, receive, maintain, or transmit EPHI on your behalf • **Require** business associates to protect EPHI by implementing safeguards that maintain the confidentiality, integrity, and availability of EPHI			
? Can you identify business associates of your organization ?	☐ **Yes**	☐ **No**	☐ **SW**
R ***THE BUSINESS ASSOCIATE CONTRACT*** **§164.308 (b) (1)** • **Require** organizations and their subcontractors that create, receive, maintain, or transmit EPHI on your behalf to sign a Business Associate Contract ○ The Business Associate Contract may already exist for your organization as part of compliance with the privacy standards			
? Do you require business associates to sign a Business Associate Contract ?	☐ **Yes**	☐ **No**	☐ **SW**

Physical Safeguards

§164.310 (a) (1) FACILITY ACCESS CONTROLS – Standard 1

Implement policies and procedures to limit physical access to your electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes	N = No	SW = Somewhat
A ***CONTINGENCY OPERATIONS*** **§164.310 (a) (2) (i)**			
• **Establish** procedures that allow select workforce members access to the facility in support of restoring lost EPHI in the event of an emergency • **Provide** appropriate access training to critical workforce members			
? Have you identified your critical workforce members in the event of a disaster ?	☐ Yes	☐ No	☐ SW
A ***FACILITY SECURITY PLAN*** **§164.310 (a) (2) (ii)**			
• **Identify** all physical locations of EPHI including, offices, computer workstations, etc. • **Implement** measures for securing locations where EPHI is stored or used • **Restrict** access to information technology system(s) to only select workforce members			
? Are your computer systems in a secure location within your organization ?	☐ Yes	☐ No	☐ SW
A ***ACCESS CONTROL AND VALIDATION PROCEDURES*** **§164.310 (a) (2) (iii)**			
• **Determine** workforce access requirements to facilities, locations, etc., where EPHI is stored and/or maintained • **Implement** appropriate workforce access controls such as key locks, swipe cards, etc. to locations where EPHI is stored and/or maintained			
? Is access to your computer systems hardware limited to select personnel ?	☐ Yes	☐ No	☐ SW
A ***MAINTENANCE RECORDS*** **§164.310 (a) (2) (iv)**			
• **Implement** tracking logs of repairs to your computer system(s) and facility that include a record of when locks are changed, security systems are replaced or modified, or offices renovated			
? Do you track maintenance activity to your facility and computer system(s) ?	☐ Yes	☐ No	☐ SW

Physical Safeguards

§164.310 (b) WORKSTATION USE – Standard 2

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***WORKSTATION USE*** **§164.310 (b)** • **Identify** EPHI available at each workstation, workforce access to each workstation, and whether each workstation interfaces with the Internet, a modem, or is a direct connect to payers • **Determine** potential security vulnerabilities at each workstation based upon EPHI it can access • **Implement** appropriate measures to protect the security of each workstation(s) that include logging off when the workstation is unattended and at the end of the work day			
? Are you aware of software applications that exist on each of your workstations ?	☐ **Yes**	☐ **No**	☐ **SW**

Physical Safeguards

§164.310 (c) WORKSTATION SECURITY – Standard 3

Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***WORKSTATION SECURITY*** **§164.310 (c)** • **Safeguard** workstations that allow access to EPHI, such as locating workstations in a locked room, positioning workstation(s) so that it cannot be accessed or viewed by unauthorized personnel			
? Are your workstations set up to require user access using a logon ID and password ?	☐ **Yes**	☐ **No**	☐ **SW**

Physical Safeguards

§164.310 (d) (1) DEVICE AND MEDIA CONTROLS – Standard 4

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***MEDIA CONTROLS & DISPOSAL*** **§164.310 (d) (2) (i)** • **Implement** measures to govern the receipt and removal of hardware and software • **Establish** criteria to destroy EPHI stored and maintained on computer system(s) hard drives, floppy discs, CDs, and other electronic media such as the use of scrubbing software or physical destruction			
? Does your organization physically destroy electronic media before disgarding ?	☐ Yes	☐ No	☐ SW
R ***MEDIA RE-USE*** **§164.310 (d) (2) (ii)** • **Eliminate** EPHI from media using scrubbing software before its reused, reformatting is not sufficient to destroy EPHI			
? Do you use some sort of scrubbing software on electronic media before reusing ?	☐ Yes	☐ No	☐ SW
A ***ACCOUNTABILITY*** **§164.310 (d) (2) (iii)** • **Identify** a member of your workforce responsible for overseeing the receipt and removal of hardware and EPHI			
? Does a member of your workforce oversee the removal of EPHI ?	☐ Yes	☐ No	☐ SW
A ***DATA BACKUP AND STORAGE*** **§164.310 (d) (2) (iv)** • **Routinely** backup information technology system(s) containing EPHI before making changes to your system(s) • **Periodically** attempt to restore backups containing EPHI in a test environment to identify potential restoration problems in electronic media or hardware • **Maintain** an onsite backup file(s) for daily/weekly time periods and store monthly backups off site			
? Do you complete a system backup prior to making hardware changes ?	☐ Yes	☐ No	☐ SW

Technical Safeguards

§164.312 (a) (1) ACCESS CONTROL – Standard 1

Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights (as specified under Administrative Safeguards, Information Access Management).

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes	N = No	SW = Somewhat
R ***UNIQUE USER IDENTIFICATION*** **§164.312 (a) (2) (i)**			
• **Limit** access to EPHI to workforce members that have been granted access rights • **Determine** individuals or positions that require access to information technology system(s) where EPHI is maintained • **Implement** procedures for identifying and tracking user identity			
? Does a procedure exist for tracking the identity of system users ?	☐ Yes	☐ No	☐ SW
R ***EMERGENCY ACCESS PROCEDURE*** **§164.312 (a) (2) (ii)**			
▪ **Establish** a process for obtaining EPHI during an emergency ▪ **Identify** workforce member(s) responsible that have access to EPHI in an emergency			
? Does your workforce know how to obtain EPHI in an emergency ?	☐ Yes	☐ No	☐ SW
A ***AUTOMATIC LOGOFF*** **§164.312 (a) (2) (iii)**			
▪ **Determine** whether your information technology system(s) have an automatic logoff feature ▪ **Establish** automatic logoff procedures best suited for your workforce ▪ **Use** screen saver options when automatic logoff feature is not available			
? Does your computer automatically logoff users after a period of inactivity ?	☐ Yes	☐ No	☐ SW

Technical Safeguards

§164.312 (a) (1) ACCESS CONTROL – Standard 1 *(continued)*

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
A ***ENCRYPTION AND DECRYPTION*** **§164.312 (a) (2) (iv)** ▪ **Determine** the risk of EPHI stored or maintained that is vulnerable to access from unauthorized users ▪ **Implement** encryption software of stored EPHI if the risk of access is unacceptable to your organization **? Have you considered your risk and the need for encrypting stored EPHI ?**	☐ **Yes**	☐ **No**	☐ **SW**

Technical Safeguards

§164.312 (b) AUDIT CONTROLS – Standard 2

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***SECURITY ASSESSMENT REVIEW*** **§164.312 (b)** • **Determine** activity tracking capabilities of your information technology system(s) that contain EPHI • **Implement** information technology system(s) activity reports where EPHI is stored and or maintained • **Evaluate** your need to install tracking software in the event your computer system(s) does not have an audit feature • **Consider** limiting access to your workforce to only select information contained in EPHI which is required to perform specific job duties • **Assign** responsibility to a member of your workforce for completing security audits on a routine basis using your risk analysis to determine appropriate level of audit controls			
? Have you implemented audit controls on your computer system(s) ?	☐ **Yes**	☐ **No**	☐ **SW**

Technical Safeguards

§164.312 (c) (1) INTEGRITY – Standard 3

Implement policies and procedures to protect EPHI from improper alteration or destruction.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
A ***MECHANISM TO AUTHENTICATE EPHI*** **§164.312 (c) (2)** • **Implement** a mechanism to validate that EPHI you transmit or receive has not been altered or destroyed such as: ○ *Installation* of a firewall on your computer(s) or network server(s) ○ *Encryption software* ○ *Host-based intrusion monitoring or detection software* ○ *Virus protection software*			
? Does your organization validate EPHI it receives electronically ?	☐ **Yes**	☐ **No**	☐ **SW**

Technical Safeguards

§164.312 (d) PERSON OR ENTITY AUTHENTICATION – Standard 4

Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
R ***PERSON OR ENTITY AUTHENTICATION*** **§164.312 (d)** • **Implement** measures to confirm that individuals granted access to EPHI are appropriately identified such as: ○ Require a password or PIN (personal identification number) to access applications or systems containing EPHI ○ Use physical devices for Internet access such as smart cards, cards with magnetic strips that store information, or one-time passwords, soft tokens, etc. ○ Biometric devices, such as fingerprints, retinal scans, or voice activation are examples of more technologically advanced authentication systems			
? Does your organization validate users before granting access to computer system(s) ?	☐ **Yes**	☐ **No**	☐ **SW**

Technical Safeguards

§164.312 (e) (1) TRANSMISSION SECURITY – Standard 5

Implement technical security measures to guard against unauthorized access to EPHI transmitted over an electronic communications network.

ⓘ Action Items & Assessment Questions	SECURITY READINESS Y = Yes N = No SW = Somewhat		
A ***PROTECTIONS & INTEGRITY CONTROLS*** **§164.312 (e) (2) (i)**			
• **Implement** data tracking logs, data modification reports, or other measures to monitor that electronically transmitted EPHI was not improperly modified • **Identify** report tracking activities to guard against improper access to EPHI transmitted over an electronic communications network			
? Does your organization monitor data access logs relating to EPHI ?	☐ Yes	☐ No	☐ SW
A ***ENCRYPTION*** **§164.312 (e) (2) (ii)**			

• **Evaluate** the need based upon actual or perceived risk for encryption technology in your organization
  ○ Exposed electronic transmission does not include "point-to-point" or "dedicated" transmission over dial-up lines or use of a modem
  ○ Transmissions using the Internet, including FTP services and bulletin boards, is susceptible to the threat of interception and risk of disclosure			

? Has your organization considered its risks to unencrypted EPHI ?	☐ Yes	☐ No	☐ SW

SECURITY READINESS
SELF ASSESSMENT INDICATOR

Count the number of "Yes" responses & circle on scale below

Required Implementation Specifications

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

Does Not Exist — **Somewhat In Place** — **Fully Implemented**

Addressable Implementation Specifications

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

Does Not Exist — **Somewhat In Place** — **Fully Implemented**

Overall, I would consider my organization to be:

_____ **Mostly compliant** with the HIPAA security requirements

_____ **Somewhat compliant** with the HIPAA security requirements

_____ **Not at all compliant** with the HIPAA security requirements

ACKNOWLEDGEMENTS

The Maryland Health Care Commission (MHCC) appreciates the input from its EDI/HIPAA Workgroup in developing the *HIPAA Security Standards, A Guide to Security Readiness.* Consultative support on the content was provided by Bill Dobson of Trustwave, and Jama Allers of MedChi. MHCC's Irene Battalen is credited with the conceptual design and general substance of the guide.

The Center for Health Information Technology
David Sharp, Ph.D.
Director

Website: www.mhcc.maryland.gov
Tel. (410)764-33460 Fax (410)358-1236